POWER RESIDUES

KAORU MOTOSE

Dedicated to professors Kazuo Kishimoto, Takasi Nagahara and Hisao Tominaga for their support

ABSTRACT. We present improved reports about the Feit Thompson conjecture until now and some new results for a prime 5.

Key Words: Feit Thompson conjecture, power residue symbol, Eisenstein reciprocity law, common index divisors.
2000 *Mathematics Subject Classification*: Primary 11A15, 11R04; Secondary 20D05.

Let $p < q$ be primes and we set

$$f := \frac{q^p - 1}{q - 1} \text{ and } t := \frac{p^q - 1}{p - 1}.$$

Feit and Thompson [5] conjectured that f never divides t. If it would be proved, the proof of their odd order theorem [6] would be greatly simplified (see [1] and [7]).
The inequality $f < t$ may be trivial but here we confirm this as follows: It is easy for $p = 2$ from $2^q > q + 2$ by $q \geq 3$. Noting $\dfrac{x}{\log x}$ is strict increasing for $x \geq 3$, we have $\dfrac{q}{\log q} > \dfrac{p}{\log p}$ and hence $p^q > q^p$ by $q > p \geq 3$. Thus we have

$$\frac{p^q - 1}{p - 1} > \frac{p^q - 1}{q - 1} > \frac{q^p - 1}{q - 1} \text{ for } q > p \geq 3.$$

If $q \equiv 1 \bmod p$, in particular $p = 2$, then f never divides t. In fact, $f\ell = t$ implies a contradiction as follows:

$$1 \equiv t = f\ell = (q^{p-1} + \cdots + 1)\ell \equiv p\ell \equiv 0 \bmod p.$$

Contrary to the simple proof, this is important and fundamental in our discussions and it shall be freely used without previous notices. In this paper, small Latin letters represent integers in case no proviso and we use very often the notation $s \overset{p}{=} t$ in stead of $s \equiv t \bmod p$.

1. COMMON PRIME DIVISORS OF f AND t

Using computer and Proposition 1,(2), Stephans [15] found that f and t have a greatest common (prime) divisor $112643 = 2pq + 1$ for primes $p = 17$ and $q = 3313$. This example is so far of the only one with a common divisor $(f, t) > 1$. In case $p = 2$, $(f, t) = 1$. In fact, if r is a common prime divisor of $f = q + 1$ and $t = 2^q - 1$, then r is odd and q is the order of 2 mod r. Hence $r \equiv 1 \bmod q$ by Fermat little theorem. This implies a contradiction $r \leqq q + 1 < r$ since r is odd.

The paper is in a final form and no version of it will be submitted for publication elsewhere.

The next Proposition 1 follows in the range of rational integers.

Proposition 1 ([15], [4] and [11])**.** *Assume r is a common prime divisor of f and t. Then we have*

(1) *p is the order of q $\mathrm{mod}\ r$ and q is the order of p $\mathrm{mod}\ r$*
(2) $r \equiv 1 \bmod 2pq$.
(3) *If $p \equiv 3 \bmod 4$ or $q \equiv 3 \bmod 4$, then $r \equiv 1 \bmod 4$.*
(4) *If $p \equiv 3 \bmod 4$ and $q \equiv 1 \bmod 4$, then f never divides t.*

Proof. (1): It follows from the assumption that $q^p \equiv 1 \bmod r$ and $p^q \equiv 1 \bmod r$. If $q \equiv 1 \bmod r$, then $0 \equiv f = q^{p-1} + \cdots + 1 \equiv p \bmod r$ and so $r = p$, which implies a contradiction $0 \equiv t \equiv 1 \bmod p$. Similarly, we have $p \not\equiv 1 \bmod r$.
(2): Since p is odd, f and r are odd. Thus (2) follows from (1) and Fermat little theorem.
(3): Let λ_p be the Legendre symbol by p. Since $\lambda_r(p) = 1$ by $p^q \equiv 1 \bmod r$ and $\lambda_p(r) = 1$ by (2), the quadratic reciprocity $1 = \lambda_r(p)\lambda_p(r) = (-1)^{\frac{p-1}{2}\frac{r-1}{2}} = (-1)^{\frac{r-1}{2}}$ shows our result for p and similarly for q.
(4): Using (3), we have a contradiction $1 \equiv f = q^{p-1} + \cdots + q + 1 \equiv p \equiv 3 \bmod 4$. □

2. Results using Eisenstein reciprocity law

We set $\zeta = e^{\frac{2\pi i}{p}}$ for odd prime p and $\eta := \zeta^c(\zeta - q)$ where $c(q-1) \overset{p}{=} 1$. Then η is primary prime (see [9, p.206]) and $f = \prod_{\sigma \in G} \eta^\sigma = N(\eta)$ where G is the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$.
We consider an integer $g := \sum_{a=1}^{p-1} \lambda_p(a) q^a$ for the Gauss sum $g(\lambda_p) = \sum_{a=1}^{p-1} \lambda_p(a)\zeta_p^a$ where $\lambda_p(a)$ is the Legendre symbol by p. Then we have $g \overset{\eta}{=} g(\lambda_p)$. More strongly, $g^2 \overset{f}{=} (-1)^{\frac{p-1}{2}} p$ by a computation using $q^p \equiv 1 \bmod f$ as that of $g(\lambda_p)^2$. The next is easy from the definition of p-th power residue symbol (see [9, p.205]).

Lemma 2. *Let χ_A be the p-th power residue symbol by an integral ideal $A \not\ni p$ of $\mathbb{Q}(\zeta)$.*

(a) $\chi_A(-1) = 1$.
(b) $\chi_\alpha(\beta) = 1$ *where α, β are real and non unit elements in $\mathbb{Q}(\zeta)$.*
(c) $\chi_A(\zeta) = \zeta^{\frac{N(A)-1}{p}}$.

Proof. (a): It follows from $\chi_A(-1) = \chi_A((-1)^p) = \chi_A(-1)^p = 1$.
(b): $\chi_\alpha(\beta)$ is real by $\overline{\chi_\alpha(\beta)} = \chi_{\bar{\alpha}}(\bar{\beta}) = \chi_\alpha(\beta)$, where $^-$ is a complex conjugate. 1 is the only real root of $x^p = 1$ for odd p.
(c): If $a \equiv 1$ and $b \equiv 1 \bmod p$, then it follows from $(a-1)(b-1) \equiv 0 \bmod p^2$ that

$$\frac{ab-1}{p} \equiv \frac{a-1}{p} + \frac{b-1}{p} \bmod p.$$

Thus if $\chi_B(\zeta) = \zeta^{\frac{N(B)-1}{p}}$ and $\chi_C(\zeta) = \zeta^{\frac{N(C)-1}{p}}$, then $\chi_{BC}(\zeta) = \zeta^{\frac{N(BC)-1}{p}}$ by $N(BC) = N(B)N(C)$. In case A is prime, (c) is clear by $A \not\supset (p) = (1-\zeta)^{p-1}$ and in general case, it follows from the above. □

The Eisenstein reciprocity law (see [9, p.207]) is used freely in this section.

Theorem 3 (Eisenstein). *$\chi_\alpha(b) = \chi_b(\alpha)$ for a primary $\alpha \in \mathbb{Q}(\zeta)$ and $b \in \mathbb{Z}$ such that p, α and b are relatively prime to each other.*

For $p = 3$, we have the next results.

Proposition 4. *Assume $p = 3$ and f divides t.*

(1) $f = q^2 + q + 1$ *is prime.*
(2) $\chi_\eta(g) = 1$.
(3) $f \overset{4}{=} 1$.
(4) $q \equiv -1 \bmod 72$.

Proof. (1) : If f is composite, then we have a contradiction $(q+1)^2 < f = q^2 + q + 1$ using Proposition 1,(2) (see [4] and [11]).
(2): Since $\chi_\eta(-1) = 1$ by Lemma 2,(a) and $\chi_\eta(3)^q = \chi_\eta(3^q) = 1$, we have the next by $q \equiv -1 \bmod 3$.

$$\chi_\eta(g)^2 = \chi_\eta(g(\lambda_3)^2) = \chi_\eta(-1)\chi_\eta(3) = 1.$$

(3): Since $g^2 \overset{f}{=} -3$ and $\lambda_f(3) = \lambda_f(3)^q = \lambda_f(3^q) = 1$, we have

$$1 = \lambda_f(g^2) = \lambda_f(-1)\lambda_f(3) = (-1)^{\frac{f-1}{2}} \text{ (see [4] and [11]).}$$

(4): $f = q^2+q+1$ is prime by (1) and $(3, f) = 1$ by Proposition 1, (2). Thus $(f, g) = 1$ since $g^2 \overset{f}{=} -3$ and so using the quadratic reciprocity on Jacobi symbols and $g = q-q^2 \overset{f}{=} 2q+1$, we have the next from $q \overset{12}{=} -1$ by (3) that

$$\begin{aligned}
\lambda_f(g) &= \lambda_f(2q+1) = (-1)^{\frac{q^2(q+1)}{2}}\lambda_{2q+1}(f) \\
&= \lambda_{2q+1}(4f) = \lambda_{2q+1}((2q+1)^2+3) \\
&= \lambda_{2q+1}(3) = (-1)^q\lambda_3(2q+1) = -\lambda_3(-1) \\
&= 1.
\end{aligned}$$

Thus $g \equiv a^2 \bmod f$ for some $a \in \mathbb{Z}$ and $(a, f) = 1$. Hence $-3 \equiv g^2 \equiv a^4 \bmod f$ and

$$1 \equiv a^{f-1} \equiv (-3)^{\frac{f-1}{4}} = (-3^q)^{\frac{q+1}{4}} \equiv (-1)^{\frac{q+1}{4}} \bmod f.$$

Therefore $q \equiv -1 \bmod 8$ (see [4], [3], [8] and [16] in this order).
Using cubic reciprocity or Eisenstein reciprocity law and Lemma 2, we have the next by (2).

$$\begin{aligned}
1 &= \chi_\eta(g)^2 = \chi_\eta(2q+1)^2 = \chi_{2q+1}(\eta)^2 \\
&= \chi_{2q+1}(\omega)^2 \cdot \chi_{2q+1}((\omega+1/2)^2) \\
&= \omega^{2((2q+1)^2-1)/3} \cdot \chi_{2q+1}(-3/4) = \omega^{2((2q+1)^2-1)/3}
\end{aligned}$$

where $\omega = e^{\frac{2\pi i}{3}}$. Hence $8q(q+1) \equiv 0 \bmod 9$ (see [12]). □

For $p = 5$, we have new results.

Proposition 5. *If $p = 5$ and f divides t, then $q \overset{25}{=} -1$ or $q \overset{25}{=} 2$ or $q \overset{25}{=} 1/2$.*

Proof. It follows from $g = q(q-1)^2(q+1)$ that

$$1 = \chi_\eta(g)^{2(q-1)} = \{\chi_\eta(q)\chi_\eta(q-1)^2\chi_\eta(q+1)\}^{2(q-1)}$$

and using freely Eisenstein reciprocity law (Theorem 3) and Lemma 2, the equations (2.1), (2.2), (2.3) follow from each computation in the last of the proof.

$$\chi_\eta(q)^{2(q-1)} = \zeta^{2q\cdot\frac{q^4-1}{5}} \tag{2.1}$$

$$\chi_\eta(q-1)^{4(q-1)} = \zeta^{2(q+1)\cdot\frac{(q-1)^4-1}{5}} \tag{2.2}$$

$$\chi_\eta(q+1)^{2(q-1)} = \begin{cases} 1 & \text{if } q \overset{5}{=} -1 \\ \zeta^{(q+1)\cdot\frac{(q+1)^4-1}{5}} & \text{if } q \overset{5}{\neq} -1 \end{cases} \tag{2.3}$$

<u>In case $q \overset{5}{=} -1$</u>, since values are 1 in (2.2) and (2.3), we obtain $2q(q^4-1) \overset{25}{=} 0$ by the power of ζ in (2.1) and so $q \overset{25}{=} -1$ by $2q(q-1)(q^2+1) \overset{5}{\neq} 0$ using $q \overset{5}{=} -1$.
<u>In case $q \overset{5}{\neq} -1$</u>, considering the power of ζ,

$$2q(q^4-1) + 2(q+1)((q-1)^4-1) + (q+1)((q+1)^4-1) \overset{25}{=} 0.$$

It follows from the above and $q(q+1) \overset{5}{\neq} 0$ that

$$5q^3 - 6q^2 - 5q - 6 \overset{25}{=} 0.$$

This has solutions $q \overset{25}{=} 2$ or $q \overset{25}{=} 1/2$.
The computation of (2.1).

$$\chi_\eta(q)^{2(q-1)} = \chi_q(\eta)^{2(q-1)} = \chi_q(\zeta^{c+1})^{2(q-1)} = \zeta^{2q\cdot\frac{q^4-1}{5}}.$$

The computation of (2.2).

$$\begin{aligned}
\chi_\eta(q-1)^{4(q-1)} &= \chi_{q-1}(\eta)^{4(q-1)} \\
&= \chi_{q-1}(\zeta^c)^{4(q-1)}\chi_{q-1}(\zeta-1)^{4(q-1)} \\
&= \chi_{q-1}(\zeta^4)\chi_{q-1}(\zeta-1)^{4(q-1)} \\
&= \chi_{q-1}(\zeta^{2(q+1)})\chi_{q-1}(\zeta-2+\zeta^{-1})^{2(q-1)} \\
&= \zeta^{2(q+1)\cdot\frac{(q-1)^4-1}{5}}.
\end{aligned}$$

The computation of (2.3). In case $q \overset{5}{=} -1$, setting s by $q+1 = 5^e s$ and $(s,5) = 1$, we have

$$\begin{aligned}
\chi_\eta(q+1)^{2(q-1)} &= \chi_s(\eta)^{2(q-1)} \\
&= \chi_s(\zeta^c)^{2(q-1)}\chi_s(\zeta+1)^{2(q-1)} \\
&= \chi_s(\zeta^2)\chi_s(\zeta+1)^{2(q-1)} \\
&= \chi_s(\zeta)^{q+1}\chi_s(\zeta+2+\zeta^{-1})^{q-1} = 1.
\end{aligned}$$

In case $q \overset{5}{\neq} -1$,

$$\begin{aligned}\chi_\eta(q+1)^{2(q-1)} &= \chi_{q+1}(\zeta^c)^{2(q-1)}\chi_{q+1}(\zeta+1)^{2(q-1)}\\ &= \chi_{q+1}(\zeta^2)\chi_{q+1}(\zeta+1)^{2(q-1)}\\ &= \chi_{q+1}(\zeta^{q+1})\chi_{q+1}(\zeta+2+\zeta^{-1})^{(q-1)}\\ &= \zeta^{(q+1)\cdot\frac{(q+1)^4-1}{5}}. \qquad \square\end{aligned}$$

3. Common index divisors

Let $F = \mathbb{Q}(\mu)$ be a number field of dimension m over $\mathbb{Q}$ and let D_F be the integer ring of F. We set $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_m) := |\alpha_k^{(\ell)}|$ where $\alpha_k^{(\ell)}$ $(0 \leqq \ell \leqq m-1)$ are conjugates of $\alpha_k \in F$ $(1 \leqq k \leqq m)$.
For an integral basis $\eta_1, \eta_2, \cdots, \eta_m$ of D_F, $d(F) := \Delta(\eta_1, \eta_2, \cdots, \eta_m)^2$ is called the discriminant of F. For $\alpha \in F$, $d(\alpha) := \Delta(1, \alpha, \alpha^2, \cdots, \alpha^{m-1})^2$ is also called the discriminant of α. It is easy to see $d(\alpha) = I(\alpha)^2 d(F)$ where $I(\alpha) \in \mathbb{Z}$.
A prime number p is called a common index divisor of F if p divides $I(\gamma)$ for all $\gamma \in D_F$.

Example 6. (1) (Dedekind) :
$h(x) = x^3 + x^2 - 2x + 8$ is irreducible over $\mathbb{Q}$. Let α be a root. Then $d(\alpha) = -2^2 \cdot 503$, $d(\mathbb{Q}(\alpha)) = -503$, $I(\alpha) = 2$, and 2 is a common index divisor of $\mathbb{Q}(\alpha)$. The Galois group of $h(x)$ is the symmetric group S_3 of degree 3.
(2) (Stephans): Both 17 and 3313 are common index divisors in some subfields of $\mathbb{Q}(\zeta_r)$ where $r = 112643$ and $\zeta_r = e^{\frac{2\pi i}{r}}$.

In general, $n > p$ for a prime p if and only if there exists a number field K of degree n such that a prime p is a common index divisor of K (see [17] for 'if' part and [2] for 'only if' part).

4. Reviews from Ireland and Rosen [9]

Using the same notations in section 1, we note that $(f, p-1) = 1$. In fact, if ℓ is a prime common divisor of f and $p-1$, then $q^p \overset{\ell}{=} 1$ and $\ell < p$. We obtain p is the order of $q \mod \ell$ since $q \overset{\ell}{=} 1$ implies a contradiction $0 \overset{\ell}{=} f = q^{p-1} + \cdots + q + 1 \overset{\ell}{=} p \overset{\ell}{=} 1$. Thus $\ell \overset{p}{=} 1$ contradicts to $\ell < p$. Hence $f \mid t$ if and only if $p^q \overset{f}{=} 1$.
From this, we remember the next well known assertion. In the text books on the elementary number theory, we can usually see that for an odd prime r and a divisor n of $r-1$, an equation $x^n \overset{r}{=} a$ is solvable if and only if $a^{\frac{r-1}{n}} \overset{r}{=} 1$. This assertion is just the Euler's criterion for $n = 2$ and the existence of primitive roots is essential in this proof.
In this section, we shall observe [9, p.197, Corollary] is a generalization of this and an improvement of [13, Theorem] by Artin map (see [14]).
Considering in general $a^n \overset{m}{=} 1$, we may assume without loss generality n is the order of $a \bmod m$ and a is a prime by Dirichlet theorem, since there exist infinite many prime numbers p with $p \overset{m}{=} a$ because a and m are relatively prime. Thus we consider here the congruence $p^n \overset{m}{=} 1$ where p is a prime and n is the order of $p \bmod m$.

This section is almost all rewrite of [9, p.196-197] with a slight improvement. Here we set p is prime, D is the integer ring of $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{\frac{2\pi i}{m}}$, and P is a prime ideal of D containing p.

The following Lemma is essential in this section. Lemma 7 and Corollary 8 were stated in [9, p.196].

Lemma 7. *If p does not divide m, then $D \equiv \mathbb{Z}[\zeta_m] \bmod p$.*

Proof. We set $\zeta = \zeta_m$ Since $\{1, \zeta, \dots, \zeta^{\varphi(m)-1}\}$ is a basis of K over $\mathbb{Q}$, we obtain $D \ni \alpha = \sum r_k \zeta^k$ where $r_k \in \mathbb{Q}$. Thus $\mathrm{Tr}(\alpha\zeta^\ell) = \sum r_k \mathrm{Tr}(\zeta^k\zeta^\ell)$, where Tr is the trace from K to $\mathbb{Q}$. Solving this linear equations about r_k, we have $dr_k \in \mathbb{Z}$, namely, $dD \subset \mathbb{Z}[\zeta]$ where $d = |\mathrm{Tr}(\zeta^k\zeta^\ell)|$ is the discriminant of a cyclotomic polynomial $\Phi_m(x)$ of order m. If $d \overset{p}{=} 0$, then $\Phi_m(x)$ has a multiple root α in D/P and hence $\Phi_m(\alpha) = 0$ and $\Phi'_m(\alpha) = 0$. Substituting α in the differential $mx^{m-1} = \Phi_m(x)'g(x) + \Phi_m(x)g(x)'$ of $x^m - 1 = \Phi_m(x)g(x)$, we have $m\alpha^{m-1} = 0$ and $\alpha = 0$ by the condition, which yields a contradiction $0 = \Phi_m(\alpha) = \Phi_m(0) = \pm 1$. Thus we have $d \underset{p}{\neq} 0$ and $D \equiv \mathbb{Z}[\zeta] \mod p$. $\square$

It is easy to see for $(a, m) = 1$, $\sigma_a : \zeta_m \to \zeta_m^a$ are automorphisms of K and $G = \{\sigma_a \mid 1 \leqq a < m,\ (a, m) = 1\}$ is the Galois group of K over $\mathbb{Q}$.

Corollary 8. (1) *$\alpha^{\sigma_p} \overset{p}{=} \alpha^p$ for $\alpha \in D$.*
(2) *$P^{\sigma_p} = P$.*
(3) *p is unramified in D.*

Proof. We set $\zeta = \zeta_m$. There exists $\beta \in D$ with $\alpha = p\beta + \sum a_k \zeta^k$ by Lemma 7.
(1) follows from

$$\alpha^{\sigma_p} = p\beta^{\sigma_p} + \sum_k a_k \zeta^{pk} \overset{p}{=} \sum_k a_k^p \zeta^{pk} \overset{p}{=} \alpha^p.$$

(2): For $\mu \in P$, $\mu^{\sigma_p} \overset{p}{=} \mu^p \overset{P}{=} 0$ and so $\mu^{\sigma_p} \in P$. This implies $P^{\sigma_p} \subset P$ and hence $P^{\sigma_p^{-1}} = P^{\sigma_p^{n-1}} \subset P$ where n is the order of σ_p.
(3): Let P be a prime ideal with $p \in P^2$ and let $\nu \in P$ but $\nu \notin P^2$. Then for the order n of σ_p, $\nu = \nu^{\sigma_p^n} \overset{p}{=} \nu^{p^n} \overset{P^2}{=} 0$ by (1) and $p^n \geqq 2$. Hence we have a contradiction $\nu \in P^2$ from $p \in P^2$. $\square$

The next Lemma 9,(1) is restated of [9, p.182].

Lemma 9. (1) *G is transitive on the set Ω of distinct prime ideals of D containing p.*
(2) *$p^{|G_P|}$ is the order of D/P, namely, $|G_P|$ is a degree of P where G_P is the stabilizer of P.*

Proof. (1): Assume there exists $Q \in \Omega$ with $Q \neq P^\sigma$ for all $\sigma \in G$. Then there exists an element α satisfying $\alpha \equiv 0 \bmod Q$ and $\alpha \equiv 1 \bmod P^\sigma$ for all $\sigma \in G$. $N(\alpha) := \prod_{\sigma \in G} \alpha^\sigma \in \mathbb{Z} \cap Q = p\mathbb{Z} \subset P$ and so a contradiction $\alpha^\tau \in P$ for some τ, namely $\alpha \in P^{\tau^{-1}}$.
(2): We set d is the degree of P and $c = |\Omega|$. Then $d = |G_P|$ follows from $cd = \varphi(m) = |G| = |G : G_P||G_P| = c|G_P|$ since p is unramified by Corollary 8,(3).

We set L is the fixed subfield of K by σ_p. The next is just [9, p.197, Corollary] and contains [13, Theorem] which follows from Artin map (see [14, p.96]).

Theorem 10. $G_P = \langle \sigma_p \rangle$.

Proof. We set that n is the order of σ_p, $d = |G_P|$ and $\langle \nu \rangle = (D/P)^\times$. Then n is divisor of d since $\langle \sigma_p \rangle \subset G_P$ by Corollary 8,(2). On the other hand $p^d - 1$ is the order of ν by lemma 9,(2) and so $p^d - 1$ is a divisor of $p^n - 1$ since $\nu = \nu^{\sigma_p^n} = \nu^{p^n}$ by Corollary 8,(1) and hence $\nu^{p^n - 1} = 1$. It is false for $n < d$ and so $n = d$. $\square$

Theorem 10 is an extension of the next familiar theorem in elementary number theory. *If r is prime and n is a divisor of $r-1$, then $p^n \overset{r}{=} 1$ if and only if $p \overset{r}{=} x^{\frac{r-1}{n}}$ is solvable.* In fact, Assume $p^n \overset{r}{=} 1$. Then we may assume n is the order of σ_p and $\langle \sigma_p \rangle = \langle \sigma_c^{\frac{r-1}{n}} \rangle$ since the subgroup of order n is unique in the cyclic $\langle \sigma_c \rangle$ where c is a primitive root of r. Hence $p \overset{r}{=} x^{\frac{r-1}{n}}$ is solvable by $\sigma_p = \sigma_c^{\frac{(r-1)}{n}k}$ for some k. The other side is trivial.

Let D_M be the integer ring of a subfield M of K and Let P_M be prime ideal of D_M containing p.

Corollary 11. *$D/P = \mathbb{F}_{p^{|G_P|}}$ and $D_M/P_M = \mathbb{F}_p$ for any subfield M of L.*

Proof. First assertion is clear from Theorem 10. Second assertion follows from

$$\alpha^p \overset{p}{=} \alpha^{\sigma_p} = \alpha \text{ for } \alpha \in D_M \text{ and so } \alpha^p \overset{P_M}{=} \alpha. \qquad \square$$

We note that $D/P = \mathbb{F}_p$ if and only if p splits completely in D by Corollary 8,(3). The next is an extension of [13, Theorem].

Corollary 12. *Assume $p^n \overset{m}{=} 1$ and set $s = [L : \mathbb{Q}]$. Then in case $s > p$, p is a common index divisor of L and in case $p = s$, $h_\theta(x) \underset{p}{\neq} x^p - x$ has a multiple root in $\mathbb{F}_p = D_L/P_L$ where $L = \mathbb{Q}(\theta)$ and $h_\theta(x)$ is the minimal polynomial of θ over $\mathbb{Q}$.*

Proof. If there exists an element of $\mu \in D_L$ such that p does not divide $I(\mu) \in \mathbb{Z}$ where $d(\mu) = I(\mu)^2 d(L)$ for the discriminants $d(\mu)$ and $d(L)$ of μ and L, respectively. Noting that p does not divide $d(L)$ by Dedekind's theorem on discriminant (see [14, p.88, Remark 2.15]) since p is unramified in K and so in L, we have $d(\mu) \overset{p}{\neq} 0$ and so the minimal polynomial $g_\mu(x)$ of μ over $\mathbb{Q}$ has distinct roots in $\mathbb{F}_p$. Thus $s = \deg g_\mu(x) \leqq p$. In particular case $s = p$, $g_\mu(x) \overset{p}{=} x^p - x$. $\square$

We prove again Proposition 1,(3) (see [11] and [13]).

Corollary 13. *If r is a common prime divisor of f and t, then $p \equiv 1 \bmod 4$ or $r \equiv 1 \bmod 4$.*

Proof. We set $m = r$ and consider Guss sum $g(\lambda) = \sum_{k=1}^{r-1} \lambda(k) \zeta_r^k$ where λ is a quadratic character by r and $\zeta_r = e^{\frac{2\pi i}{r}}$. It is well known that $g(\lambda)^2 = (-1)^{\frac{r-1}{2}} r \overset{p}{=} (-1)^{\frac{r-1}{2}}$ and $g(\lambda) = \theta - \theta_1 = 2\theta + 1$ by $\theta + \theta_1 = -1$ where $\theta = \sum_{\lambda(a)=1} \zeta_r^a$ and $\theta_1 = \sum_{\lambda(b)=-1} \zeta_r^b$. $M = \mathbb{Q}(\theta) = \mathbb{Q}(g)$ is a quadratic subfield of L by $r \overset{2pq}{=} 1$ (see Proposition 1,(2)).

Since $\theta \overset{P_M}{\equiv} b$ for $b \in \mathbb{Z}$ by Corollary 11,

$$(-1)^{\frac{r-1}{2}\frac{p-1}{2}} \overset{p}{\equiv} g(\lambda)^{p-1} = (2\theta+1)^{p-1} \overset{P_M}{\equiv} (2b+1)^{p-1} \overset{p}{\equiv} 1.$$

Noting $2b+1 \overset{p}{\not\equiv} 0$ by above equations except the last equivalence, we can complete these from Fermat little theorem. $\square$

We prove again the part $q \overset{9}{\equiv} -1$ of Proposition 4,(4) (see [12] and [13]).

Corollary 14. *If f divides t for a prime $p=3$, then $q \overset{9}{\equiv} -1$.*

Proof. The assumption implies $q \overset{3}{\equiv} -1$ and $f = q^2+q+1$ is prime by Proposition 4. Let c be a primitive root of f and set $\zeta = e^{\frac{2\pi i}{f}}$. Then $\sigma : \zeta \to \zeta^c$ is a generator of the Galois group G of $K = \mathbb{Q}(\zeta)$ over $\mathbb{Q}$, let L_3 be the correspond subfield to $H = \langle \sigma^3 \rangle$. and let $G = \bigcup_{s=0}^{2} H\sigma^s$ be a coset decomposition by H. We set also $\theta = \sum_{\tau\in H} \zeta^\tau$ and $\theta_s = \theta^{\sigma^s}$ for $s = 0,1,2$. We can see $[L_3 : \mathbb{Q}] = 3$ and $L_3 = \mathbb{Q}(\theta)$ by [14, p.61, Theorem 2.6].
Let $g = g(\chi)$ be a cubic Gauss sum for the cubic residue character χ by a primary prime divisor $\eta = \omega(\omega - q)$ of $f = \eta\bar{\eta}$ in $\mathbb{Z}[\omega]$, where $\omega = e^{\frac{2\pi i}{3}}$. Namely, we set $g_s = g(\chi^s) = \sum_{t=0}^{f-1} \chi^s(t)\zeta^t$ which are rewritten as follow

$$g_s = \sum_{t=0}^{2}\sum_{k=0}^{\frac{f-4}{3}} \chi^s(c^{3k+t})\zeta^{c^{3k+t}} = \sum_{t=0}^{2} \chi(c)^{st}(\sum_{\tau\in H}\zeta^\tau)^{\sigma^t} = \sum_{t=0}^{2} \omega^{st}\theta_t.$$

These equations are also solved about θ_s as $3\theta_s = \sum_{t=0}^{2} \bar{\omega}^{st} g_t$. We can set the minimal polynomial $h_\theta = x^3 + x^2 + a_2 x + a_3$ of θ over $\mathbb{Z}$ by $\sum_{s=0}^{2} \theta_s = -1$.
We shall show $a_3 \overset{3}{\equiv} -a_2$. Noting [9, p.92, Proposition 8.2.2] and $\bar{\theta}_s = \theta_s$ since the complex conjugate $^-$ is the element of order 2 in H,

$$f = |g(\chi)|^2 = g(\chi)\overline{g(\chi)} = \theta_0^2 + \theta_1^2 + \theta_2^2 + (\omega+\omega^2)a_2 = 1 - 3a_2.$$

Hence we have

$$a_2 = (1-f)/3 = -q\cdot(q+1)/3 \overset{3}{\equiv} (q+1)/3.$$

It follows from equations $3\theta_s = \sum_{t=0}^{2} \bar{\omega}^{st} g_t$ that

$$-3^3 a_3 = (3\theta_0)(3\theta_1)(3\theta_2) = \prod_{s=0}^{2}(\sum_{t=0}^{2} \bar{\omega}^{st} g_t) = g_0^3 + g_1^3 + g_2^3 - 3g_0g_1g_2.$$

Using Stickelberger relation $g_1^3 = f\eta$ ([9, p.115, Corollary]), we can see the next from $g_0 = -1,\ g_2 = \bar{g}_1$ and $\eta + \bar{\eta} = q-1$.

$$-a_3 = (-1 + f(\eta+\bar{\eta}) + 3f)/3^3 = ((q+1)/3)^3 \overset{3}{\equiv} (q+1)/3 \overset{3}{\equiv} a_2.$$

Thus we have $a_3 \overset{3}{\equiv} -a_2$.
Since $h_\theta \neq x^3 - x$ has a multiple root b in $\mathbb{F}_3$ by Corollary 12, we have $h'_\theta(b) \overset{3}{\equiv} 0$, namely, $b \overset{3}{\equiv} a_2$, where $h'_\theta(x)$ is a derivative of $h_\theta(x)$. Thus $0 \overset{3}{\equiv} h_\theta(a_2) \overset{3}{\equiv} a_2 - a_2^2 + a_3 \overset{3}{\equiv} -a_2^2$ and $0 \overset{3}{\equiv} a_2 \overset{3}{\equiv} (q+1)/3$. $\square$

Example 15. If m has a primitive root, namely, $m = 2, 4, r^e$ and $2r^e$ where r is odd primes (see [9, p.44]), then G is cyclic and L_s is the unique subfield with $[L_s : \mathbb{Q}] = s$. Thus we have next results from Corollary 12.

(1) If $\ell^{r-1} \overset{r^2}{=} 1$ for primes ℓ, r with $\ell < r$, then ℓ is a common index divisor of a subfield L_r of $\mathbb{Q}(\zeta_{r^2})$.

(2) If $p^q \overset{r}{=} 1$ for primes p, r with $qq' = r-1$ and $p < q'$, then p is a common index divisor of a subfield $L_{q'}$ of $\mathbb{Q}(\zeta_r)$ (see [13, Theorem]).

Question. *If f divides t, then is f square free ?*

This question follows from the next observations: If f divides t, then we can see $p^q \equiv 1$ and $q^p \equiv 1 \bmod f$. Thus if f is divided by a prime square r^2, we have $p^{r-1} \equiv 1$, $q^{r-1} \equiv 1 \bmod r^2$ by $r \equiv 1 \bmod 2pq$ (see Proposition 1,(2)). It is well known from computation by using computer that there are rare primes r satisfying $a^{r-1} \equiv 1 \bmod r^2$ for a fixed $a > 1$. Further, in this case $p \not\equiv q \bmod r$ for fixed numbers p, q.

5. Integral normal basis

Let K be a Galois extension over $\mathbb{Q}$ with the Galois group G and let D be the integer ring of K. If there exists an element $\mu \in D$ such that $D = \sum_{\sigma\in G} \mu^\sigma \mathbb{Z}$, then we call $\{\mu^\sigma \mid \sigma \in G\}$ a normal basis and μ a normal basis element.

Here we set D_m is the integer ring of the cyclotomic field $K = \mathbb{Q}(\zeta_m)$ with the Galois group G, where $\zeta_m = e^{\frac{2\pi i}{m}}$. We set also D_θ is the integer ring of a proper subfield $\mathbb{Q}(\theta)$ of K and G_α is the stabilizer of $\alpha \in K$. In the text book [14, p.73-74], it was proved that the integer rings of subfields in $\mathbb{Q}(\zeta_r)$ for a prime r have normal bases and this plays an important role in [13]. Moreover, the integer rings of quadratic fields $\mathbb{Q}(\sqrt{n})$ have normal bases if and only if $n \equiv 1 \bmod 4$.

In the last of this paper, we shall show the following. It seems to be closely rated to the above Question.

Proposition 16. *D_m has a normal basis if and only if m is square free.*

Proof. Assume m is square free. In case m is a prime, D_m has a normal basis by [14, p.74, Remark 2.10] and so our result holds by the method in the proof of [10, p.68, Proposition 17 and p.75, Theorem 4].

Conversely, we assume D_m has a normal basis and m is divided by the square r^2 of a prime r. Then using [14, p.74, Theorem 2.12], we may assume $m = r^2$ and D_θ with $[\mathbb{Q}(\theta) : \mathbb{Q}] = r$ has a normal basis element μ. Thus we can show that $D_{r^2} = \sum_{\rho\in\ G_\omega} \mu^\rho D_\omega$ where $\omega = \zeta_{r^2}^r$. In fact, $[\mathbb{Q}(\omega) : \mathbb{Q}] = r-1$ yields $G = G_\theta \times G_\omega$ and $K = \mathbb{Q}(\theta) \cdot \mathbb{Q}(\omega) = \mathbb{Q}(\theta)[\omega] = \mathbb{Q}[\theta, \omega]$. Noting $d = \pm 1$ if α/d is an algebraic integer for an algebraic integer α and $d \in \mathbb{Z}$ with $(\alpha, d) = 1$, we obtain

$$D_{r^2} = D_\theta D_\omega = (\sum_{\nu\in G/G_\theta} \mu^\nu \mathbb{Z}) D_\omega = \sum_{\rho\in G_\omega} \mu^\rho D_\omega$$

Since D_{r^2} has a basis $\{1, \zeta, \ldots, \zeta^{\ell-1}\}$ with $\zeta = \zeta_{r^2}$ and $\ell = r^2 - r$ by $D_{r^2} = \mathbb{Z}[\zeta]$ (see [10, p.75, Theorem 3]), we have

$$\mu = \sum_{k=0}^{\ell-1} a_k \zeta^k = \sum_{t=0}^{r-1} \sum_{s=0}^{r-2} a_{rs+t} \zeta^{rs+t} = \sum_{t=0}^{r-1} \alpha_t \zeta^t \text{ where } \alpha_t = \sum_{s=0}^{r-2} a_{rs+t} \omega^s \in D_\omega.$$

We set $\tau = \sigma_b$ with $b = c^{r-1}$ where c is a primitive root for r^2. Noting $G_\omega = \langle \tau \rangle$ is the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\omega)$, we can see from this equation that

$$\mu^{\tau^s} = \sum_{k=0}^{r-1} \alpha_k \zeta^{k\tau^s} = \sum_{k=0}^{r-1} \alpha_k \omega^{k\frac{b^s-1}{r}} \zeta^k.$$

This is equivalent to

$$(\mu, \mu^\tau, \mu^{\tau^2}, \ldots, \mu^{\tau^{r-1}}) = (1, \zeta, \ldots, \zeta^{r-1})A, \text{ where } A := (\alpha_k \omega^{k\frac{b^s-1}{r}})_{k,s}.$$

The next calculation implies a contradiction such that a unit $|A|$ is contained in rD_ω. Since r is the order of $b = c^{r-1} \bmod r^2$, we have for $r > k > 0$,

$$k\frac{b^s-1}{r} \equiv k\frac{b^t-1}{r} \bmod r, \text{ i.e., } b^s \equiv b^t \bmod r^2 \text{ if and only if } s \equiv t \bmod r.$$

Thus for any $k > 0$, we obtain

$$\sum_{s=0}^{r-1} \omega^{k\frac{b^s-1}{r}} = \sum_{t=0}^{r-1} \omega^t = \frac{\omega^r - 1}{\omega - 1} = 0.$$

This equation shows that we can change the first column of $|A|$ is equal to $(r\alpha_0,\ 0,\ \cdots,\ 0)^t$ and so we have a contradiction such that a unit $|A|$ is contained in rD_ω. $\square$

We confirm Proposition 16 for $r = 2$ and Kronecker-Weber theorem for quadratic fields (see [10, p.210, Corollary 3] or [14, p.133]).

Confirmation. *The quadratic field* $\mathbb{Q}(\sqrt{n})$ *with the discriminant* d *is a subfield of* $\mathbb{Q}(\zeta_d)$.
In fact, ℓ represent primes and we set $s = {}^\#\{\ell \mid \ell \equiv -1 \bmod 4, \ell | n\}$. Using $g_\ell^2 = (-1)^{\frac{\ell-1}{2}}\ell$ in any case, where g_ℓ is a quadratic Gauss sum by ℓ, we can see our assertion.
In case $n \equiv 1 \bmod 4$, noting s is even,

$$\mathbb{Q}(\sqrt{n}) \subset \prod_{\ell|n} \mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\zeta_n).$$

In case $n \equiv -1 \bmod 4$, noting s is odd and $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$,

$$\mathbb{Q}(\sqrt{n}) \subset \mathbb{Q}(\zeta_4) \prod_{\ell|n} \mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\zeta_{4n}).$$

In case $n \equiv 2 \bmod 4$, we set $n = 2n_0$ where n_0 is odd. Noting the above two cases and $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$ by $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$,

$$\mathbb{Q}(\sqrt{n}) \subset \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{n_0}) \subset \mathbb{Q}(\zeta_8) \prod_{\ell|n_0} \mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\zeta_{4n}).$$

References

[1] Apostol, T. M., *The resultant of the cyclotomic polynomials $F_m(ax)$ and $F_n(bx)$*, Math. Comput. **29** (1975), 1-6.

[2] Bauer, M., *Über die außerwesentlichen Discriminantenteiler einer Gattung,* Math. Ann. **64** (1907) 573-576.

[3] Berndt,B. C., Evans R.J. and Williams, K. S., *Gauss and Jacobi sums,* Wiley, New York, 1998. (see p.103 and p. 231, Ex. 11)

[4] Dilcher, K. and Knauer, *J. On a conjecture of Feit and Thompson,* Fields institute communications, **41** (2004)) 169-178.

[5] Feit, W. and Thompson, J. G., *A solvability criterion for finite groups and some consequences*, Proc. Nat. Acad. Sci. USA **48** (1962), 968-970.

[6] Feit, W. and Thompson, J. G.,*Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775-1029.

[7] Guy, R. K., *Unsolved problems in number theory*, Springer, 3rd ed., 2004.

[8] Hudson, R. and Williams, K. S., *Some new residuacity criteria,* Pacific J. of Math. **91**(1980), 135-143. (see p.139, Proof of Theorem 2.)

[9] Ireland, K. and Rosen, M., *A classical introduction to modern number theory.* Springer, 2nd ed., 1990.

[10] Lang, S., *Algebraic number theory,* Addison Wesley, 1970.

[11] Motose, K., *Notes to the Feit-Thompson conjecture*, Proc. Japan, Acad., ser A, **85**(2009), 16-17.

[12] Motose, K., *Notes to the Feit-Thompson conjecture. II*, Proc. Japan, Acad., ser A, **86**(2010), 131-132.

[13] Motose, K., *The Example by Stephans* , Proc. Japan, Acad., ser A, **88**(2012), 35-37.

[14] Ono, T., *An introduction to algebraic number theory,* Plenum Press 1990 (a translation of Suron Josetsu, Shokabo, 2nd ed., 1988).

[15] Stephens, N. M., *On the Feit-Thompson conjecture*, Math. Comput. **25** (1971), 625.

[16] Whiteman, A. L., *The cyclotomic numbers of order twelve,* Acta. Arithmetica **6** (1960), 53-76. (see p.68 and the tables for the cyclotomic numbers of order 6.)

[17] von Żyliński, E., *ZurTheorie der außerwesentlichen Discriminantenteiler algebraischer Körper,* Math. Ann. **73** (1913) 273-274.

Emeritus Professor, Hirosaki University
Toriage 5-13-5, Hirosaki, 036-8171, JAPAN
E-mail address: moka.mocha_no_kaori@snow.ocn.ne.jp